

Continuation of Application for Search Warrant

I, Heather Williamson, being duly sworn, state as follows:

I. Introduction

1. I make this Continuation of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – a cellular telephone, namely, a blue Alcatel flip phone as described more fully in Attachment A (the “**Subject Device**”) used by DARRELL JONATHON MARTIN II – that is currently in the possession of law enforcement, and the extraction of electronically stored information from that property as described in Attachment B.

2. I am a Special Agent of the Drug Enforcement Administration (“DEA”) and have been so employed since January 2013. I am currently assigned to the Grand Rapids District Office. Previously, I was assigned to the Southwest Border Initiative Group-3 (“SWB-3”) and to the Los Angeles Strike Force for approximately six years. The Los Angeles Strike Force is an investigative group jointly led by the DEA and the FBI, and composed of several other federal, state, and local agencies that is focused on the disruption of the Mexico-based Sinaloa Cartel. Prior to working as a DEA Special Agent, I completed 20 weeks of training at the DEA Academy in Quantico, Virginia, which included instruction in narcotics identification, detection, trafficking, and interdiction; money laundering techniques; asset identification, seizure, and forfeiture; and techniques used by narcotics traffickers to avoid detection by law enforcement officials. I have investigated drug

trafficking organizations involved in violating various federal laws, including, but not limited to, unlawful importation of controlled substances; the distribution of controlled substances; manufacturing of controlled substances; and possession with intent to distribute controlled substances, including cocaine, methamphetamine, heroin, and other dangerous drugs; as well as money laundering. I have participated in investigations of unlawful drug trafficking and money laundering and, among other things, have conducted or participated in surveillance; execution of search warrants; debriefings of informants; reviewing of taped conversations and drug records; and have participated in investigations that include the interception of wire communications.

3. Through my training, education and experience, I have become familiar with the manner in which illegal drugs are transported, stored, and distributed, the methods of payment for such drugs, the laundering of narcotics proceeds, and the dialect (lingo) and coded language used by narcotics traffickers. In connection with my duties, I investigate criminal violations of the federal and state controlled substance laws, including, but not limited to, conspiracy and attempt to possess with intent to distribute and to distribute controlled substances, in violation of Title 21, United States Code, Section 846; possession with intent to distribute and distribution of controlled substances, in violation of Title 21, United States Code, Section 841(a)(1); use of communication facilities to facilitate drug trafficking offenses, in violation of Title 21, United States Code, Section 843(b); and offenses involving money laundering as well as conspiracy and attempt to do the same, in

violation of Title 18, United States Code, Sections 1956 and 1957. Many of these investigations also involve firearms offenses, including violations of Title 18, United States Code, Sections 922(g) and 924(c).

4. Because this Continuation is for the limited purpose of establishing probable cause to support the issuance of a search warrants for the proposed **Subject Device**, it contains only a summary of relevant facts. I have not included each and every fact known to me or to other law enforcement officers concerning the entities, individuals, and events described in this Continuation.

5. The statements contained in this Continuation are based in part on: (a) my personal participation in this investigation; (b) information provided by other federal and state law enforcement officers, including members of the Michigan State Police's West Michigan Enforcement Team (WEMET); (c) laboratory analysis reports; (d) surveillance reports; (e) criminal history records; (f) information from confidential informants; and (g) my training and experience and the training and experience of other law enforcement agents.

II. Probable Cause

A. Darrell MARTIN Historical Information

6. MARTIN is a 38-year old Muskegon, Michigan resident. MARTIN's criminal history includes a 2003 felony conviction for felon in possession of a firearm, that he served approximately 57 months in custody and 3 years supervised release. MARTIN was released from US Probation on May 24, 2011.¹ MARTIN was also

¹ As evidenced by this conviction, I know, based on my training and experience that

convicted in 2013 for delivery of marijuana and in 2019 for controlled substance possession and felony resist and obstruct arrest.

7. On January 27, 2021, MARTIN was indicted by a grand jury of the Western District of Michigan for (i) conspiracy to distribute and possess with intent to distribute 50 grams or more of methamphetamine from April 2019 to July 2020; (ii) possession with intent to distribute 50 grams or more of methamphetamine on July 13, 2020; (iii) possession with intent to distribute 50 grams or more of methamphetamine on July 28, 2020. *See United States v. Chandler, et al.*, No. 1:21-cr-00019-RJJ, R.1: PageID.1-4.

B. MARTIN Conspires with Corey CHANDLER and Dylan John FIALEK

8. MARTIN became the subject of a drug investigation in 2020, which ultimately resulted in a July 13, 2020 traffic stop where Corey CHANDLER was driving a Nissan Pathfinder carrying approximately 17 pounds of methamphetamine hidden in the inside panel of the rear cargo area of the vehicle. In the vehicle, was Corey CHANDLER, who conspired with MARTIN to purchase the methamphetamine from Arizona and transport it to Michigan. Both CHANDLER and MARTIN were indicted by the grand jury for possession with intent to distribute 50 grams or more of methamphetamine relating to this incident.

9. Dylan John FIALEK was also involved in the methamphetamine trafficking conspiracy with CHANDLER and MARTIN, but not in the Pathfinder at

firearms are common tools of the drug trade. Drug traffickers cannot communicate with law enforcement to report theft of drugs or drug proceeds and often need to carry firearms to protect their drugs and money and to protect themselves.

the time of the stop. After a guilty plea, FIALEK was convicted on February 23, 2021 in the Western District of Michigan for conspiracy to distribute 50 grams or more of methamphetamine. *See United States v. Fialek*, No. 1:20-cr-00153-RJJ, R.40: Judgement, PageID.162-168.

10. In June 2020, law enforcement received a tip from a relative of FIALEK's. The relative told law enforcement that he was aware that FIALEK dealt methamphetamine and that he encountered FIALEK at a family reunion who asked to use his phone to contact his partner, later determined to be Darrell MARTIN.²

11. FIALEK's relative told law enforcement that he received a call back from FIALEK's partner who went by the nickname "Key." According to the relative, "Key" told him that he had flown to California from Chicago and was on his way back to Michigan in a rental car with 10 kilograms of methamphetamine.³

12. On June 30, 2020, at the direction of detectives of the West Michigan Enforcement Team (WEMET), FIALEK's relative placed a call into MARTIN who then stated that he would be returning to Michigan on July 3, 2020. WEMET obtained a GPS ping warrant for MARTIN's phone, which showed the phone at a

² The number FIALEK called, (231) 726-0771, is subscribed to Darrell MARTIN. On July 28, 2020, law enforcement seized this phone from MARTIN during the possession with intent to distribute methamphetamine arrest of FIALEK and MARTIN.

³ It is unclear why MARTIN was so explicit about drug business on the phone with the relative. Text messages from MARTIN's phone, however, suggest that the relative may have had some relationship or considered being involved with MARTIN's drug trafficking business.

Double Tree hotel in Tempe, Arizona. Investigators also located a 2020 Nissan Pathfinder that was rented by Avis to Amanda DOOLEY, MARTIN's girlfriend and observed MARTIN entering and exiting the vehicle at the hotel. The Pathfinder was originally due back to Avis in Kentwood, Michigan on July 7, 2020, but DOOLEY extended the rental to July 15, 2020.

13. On July 3, 2020, GPS pings from MARTIN's phone showed that he flew back to Michigan. Homeland Security Investigation (HSI) agents in Arizona assisting law enforcement in Michigan confirmed through surveillance that the Pathfinder remained there. Pings and WEMET surveillance also showed that MARTIN boarded a plane in Grand Rapids and flew back to Arizona on July 6, 2020.

14. On July 12, 2020, GPS pings from MARTIN's phone showed that MARTIN was travelling back to Michigan. On July 13, 2020, Michigan State Police (MSP) troopers stopped the vehicle on Interstate 94 in Berrien County based on reasonable suspicion that the vehicle was carrying narcotics and for traffic violations (concealing the state of registration on the license plate and following too closely). The vehicle was driven by CHANDLER, and carried MARTIN (front seat passenger), and Jarvis Lay LESTER, a Kalamazoo resident (backseat passenger).

15. After being questioned by troopers, the passengers gave conflicting stories of their travels. For example, MARTIN said that he was heading to Texas to see a girlfriend, but went to Arizona for a few days because the state of Texas was shut down. He claimed that all three passengers met in Arizona. LESTER, however, stated that they met in Colorado, and were not in any other state other than

Colorado, where they all met up. MSP learned that MARTIN and CHANDLER had warrants for their arrest out of Muskegon. The two were ultimately not arrested because of pickup range and COVID-19 restrictions with the warrants.

16. In connection with the stop, MSP utilized a canine officer to perform a sniff of the vehicle and the canine indicated the presence of narcotics near the right rear quarter panel of the vehicle. After the canine alerted, MSP searched the vehicle on the roadside and found approximately \$13,000 in U.S. currency. MSP also found a screwdriver in the back cargo area of the vehicle, which investigators believed may have been used to access a secret compartment. MSP did not, however, locate the drugs. Law enforcement contacted Avis who requested a tow since none of the men were authorized drivers of the vehicle.

17. As MSP failed to locate the methamphetamine during the roadside search, the vehicle was removed from the roadside, and the troopers told the men to grab their belongings and that they were free to leave. Immediately after the stop, plain clothes WEMET officers who were playing a supporting role during the stop then observed the three men outside at a Five Guys restaurant in St. Joseph. WEMET officers overheard MARTIN on a call say, "the shit is still in there" and discuss the drug canine and the stop. Believing that drugs were in a secret compartment in the vehicle, investigators searched the vehicle again and found approximately 18 pounds of methamphetamine concealed in the interior panels of the rear quarter panels of the vehicle, which later lab tested positive 7,181 grams of

methamphetamine at approximately 97% purity. The methamphetamine is pictured in the trunk of the Pathfinder below:



18. Because MARTIN and CHANDLER were not present when investigators ultimately located the methamphetamine, investigators believe that they had no knowledge that the drugs were discovered and removed from the Pathfinder.

19. On July 28, 2020, law enforcement received information from an informant that FIALEK was in Muskegon County making deliveries of methamphetamine. At around 6 PM on July 28, 2020, investigators located FIALEK driving a U-Haul van with Arizona plates. Investigators surveilled FIALEK drive to a Marathon gas station in Muskegon, Michigan. FIALEK then drove to a nearby alley where he met with MARTIN, who was driving a blue Chevrolet Silverado

pickup truck. Investigators then observed MARTIN hand FIALEK a bag, which they believed to be the transfer of a package of narcotics.

20. FIALEK and MARTIN drove off separately before meeting again at another location in Muskegon. At that location, investigators observed FIALEK open and go under the hood of the U-Haul van. FIALEK closed the hood after a brief period. MARTIN then parked his Silverado. Investigators then observed FIALEK a second time, at a separate location in Muskegon, stop and exit the vehicle, and open and go under the hood.

21. Investigators continued to surveil the vehicle. Eventually, the U-Haul exited and stopped at a gas station in Muskegon, County, Michigan. Law enforcement approached the vehicle and detained both FIALEK and MARTIN, who was in the passenger seat. Law enforcement searched underneath the hood and found, in plastic shopping bags, approximately four and a half ounces (approximately 128 grams) of a crystalline substance, which lab tested as methamphetamine.

22. Investigators located the blue Silverado pickup, which MARTIN was seen driving before he delivered the bag of suspected narcotics to FIALEK, in Muskegon Heights. The truck was an Enterprise rental vehicle. Investigators contacted Enterprise; a risk team manager stated that that the vehicle was rented in a female subject's name who had reported it stolen on July 28, 2020. After MARTIN and FIALEK had been arrested in the U-Haul, investigators searched the Silverado. Investigators located **Subject Device** in the driver's side door handle of

the Silverado.⁴ Based on my training, experience, and familiarity with the investigation, I believe **Subject Device** was a second phone used by MARTIN to communicate about drug trafficking. I know that it is common for drug traffickers to use multiple phones, as they may wish to communicate with a certain subset of individuals (*e.g.*, customers, suppliers, etc.) from a different device or a device that is used only for purposes of drug trafficking.

23. MARTIN has used cellular telephones to communicate about drug trafficking. When investigators arrested MARTIN on July 28, 2020, they found a cell phone, later confirmed to be the same phone with which MARTIN initially contacted FIALEK's relative, (231) 726-0771. Law enforcement obtained a search warrant for this phone and an extraction report revealed multiple communications indicative of drug trafficking and contact with co-conspirators, CHANDLER and FIALEK.

24. **Subject Device** has been secured and maintained in the custody of the Michigan State Police in its original state. Based on my training and experience, I know that electronic data is stored for long periods of time, particularly when the device hasn't been altered, which has been the case with **Subject Device** that was seized in July 2020.

25. Therefore, there is probable cause to believe that forensic examination

⁴ On July 28, 2020, MARTIN was the sole occupant of the Silverado. Following his arrest with FIALEK, MARTIN was advised of his *Miranda* rights and admitted driving the Silverado truck. He stated that he had paid a female friend of FIALEK's to use the truck.

of the **Subject Device** will reveal electronic evidence of violations of conspiracy to distribute controlled substances in violation of Title 21, United States Code, Section 846 and possession with intent to distribute and distribution of controlled substances, in violation of Title 21, United States Code, Section 841(a)(1). The applied-for warrant would authorize the forensic examination of the **Subject Device** listed in Attachment A for the purpose of identifying electronically stored data particularly described in Attachment B. I know from training and experience that drug traffickers frequently utilize mobile telephones to facilitate drug transactions. Drug traffickers rely upon voice phone services, SMS and MMS text messaging, social media instant messaging services, and electronic mail apps to communicate with suppliers, customers, and confederates. Mobile telephones are portable and phone providers often do not require purchasers or users of the devices to provide their true names and/or addresses, so drug traffickers often maintain multiple devices to avoid detection by law enforcement. Mobile phones often contain evidence indicative of drug trafficking, including records of incoming and outgoing calls; text messages; photographs of narcotics, coconspirators, or currency; and, in the case of “smart phones,” Global Positioning System (“GPS”) data indicating the location of the device at given points in time.

26. Based on my training and experience, I know that electronic devices such as the **Subject Device**, can be used to store electronic information for long periods of times, including years. Even if a drug trafficker is being cautious of law enforcement detection and deleting the substance of communications, significant

data may still remain on the phone, such as call logs, contact information, photographs, wireless internet connections (which can reveal location information), and other location information.

27. Further, based upon my training, experience, and participation in drug investigations and financial investigations relating to drug investigations, I am aware of the following:

- a. Drug traffickers often keep names, aliases, and/or contact information of suppliers, purchasers, and others involved in drug trafficking in their devices;
- b. Drug traffickers sometimes use electronic messaging or messaging apps, in addition to MMS, SMS text messages, and voice call, to communicate with suppliers, purchasers, and others involved in drug trafficking on their devices;
- c. Drug traffickers often take pictures or videos of their drug trafficking associates, drugs, money and/or firearms, which they store on their devices;
- d. Drug traffickers often maintain, on hand, large amounts of currency in order to maintain and finance their on-going narcotics business and often store information related to the profits of their narcotics trafficking on their devices;
- e. Global Position System (GPS) data on phones may show the location of a drug trafficker at a given time, which may provide corroborating evidence of a drug delivery or other instance of drug trafficking;
- f. User attribution data and usernames, passwords, documents, and browsing history can provide evidence that the device is being used by a drug trafficker and can provide other useful evidence to the drug investigation;
- g. Drug traffickers often use the Internet to look up various information to support their drug trafficking activities on their devices;

- h. Drug traffickers often have unexplained wealth and assets as they do not have a job, nor do they report income on their state or federal tax returns. Subjects often use cash, money orders, and cashier's checks, and prepaid debit cards as a way of purchasing items as a way to disguise where the funds are ultimately coming from. Subjects will place assets in the names of nominees, which are often friends and family members in an attempt to hide the true ownership of the assets. It is common for drug traffickers to maintain books, records, receipts, notes, ledgers, receipts relating to the purchase of financial instruments and or the transfer of funds, and other papers relating to the transportation, ordering, sale and distribution of controlled substances. That the aforementioned books, records, receipts, notes, ledgers, etc., are maintained where the traffickers have ready access to them, including their devices;
- i. It is common for persons involved in drug trafficking to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and or expenditure of drug proceeds on their devices. This evidence includes information related to currency, financial instruments, precious metals and gemstones, jewelry, books, records, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashier's checks, bank checks, safe deposit box receipts or keys, records concerning storage lockers and money wrappers; and
- j. Drug traffickers frequently receive their supply of drugs through packages sent by U.S. Mail or third-party delivery service and frequently keep copies of tracking numbers, receipts and photographs of packaged narcotics on their devices.

TECHNICAL TERMS

28. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log,"

which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical

representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

29. Based on my training and experience, I believe that the **Subject Device** has capabilities that allow them to serve as a wireless telephone, digital camera,

portable media player, GPS navigation device, and/or PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

30. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Subject Device** was used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Subject Device** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion

is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

33. *Manner of execution.* Because this warrant sought in this continuation seeks only permission to examine devices should they come into law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant for search of the **Subject Device** at any time in the day or night.

V. Conclusion

34. Based on the above information, I believe that there is probable cause to search the **Subject Device**.